Proof of adjourn (PoAj)

Sayeed, Sarwar; Marco-Gisbert, Hector

Published in:
Applied Sciences

DOI:
10.3390/app10186607

Published: 22/09/2020

Document Version
Publisher's PDF, also known as Version of record

applied sciences

MDPI

Article

Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks

Sarwar Sayeed † **and Hector Marco-Gisbert** *,†

School of Computing, Engineering and Physical Sciences, University of the West of Scotland, High Street, Paisley PA1 2BE, UK; sarwar.sayeed@uws.ac.uk

* Correspondence: hector.marco@uws.ac.uk; Tel.: +44-1418494418

† Current address: High Street, Paisley PA1 2BE, UK.

Received: 19 August 2020; Accepted: 17 September 2020; Published: 22 September 2020

Abstract: The blockchain is a distributed ledger technology that is growing in importance since inception. Besides cryptocurrencies, it has also crossed its boundary inspiring various organizations, enterprises, or business establishments to adopt this technology benefiting from the most innovative security features. The decentralized and immutable aspects have been the key points that endorse blockchain as one of the most secure technologies at the present time. However, in recent times such features seemed to be faded due to new attacking techniques. One of the biggest challenges remains within the consensus protocol itself, which is an essential component to bring all network participants to an agreed state. Cryptocurrencies adopt suitable consensus protocols based on their mining requirement, and Proof of Work (PoW) is the consensus protocol that is being predominated in major cryptocurrencies. Recent consensus protocol-based attacks, such as the 51% attack, Selfish Mining, Miner Bribe Attack, Zero Confirmation Attack, and One Confirmation Attack have been demonstrated feasible. To overcome these attacks, we propose Proof of Adjourn (PoAj), a novel consensus protocol that provides strong protection regardless of attackers hashing capability. After analyzing the 5 major attacks, and current protection techniques indicating the causes of their failure, we compared the PoAj against the most widely used PoW, showing that PoAj is not only able to mitigate the 5 attacks but also attacks relying on having a large amount of hashing power. In addition, the proposed PoAj showed to be an effective approach to mitigate the processing time issue of large-sized transactions. PoAj is not tailored to any particular attack; therefore, it is effective against malicious powerful players. The proposed approach provides a strong barrier not only to current and known attacks but also to future unknown attacks based on different strategies that rely on controlling the majority of the hashing power.

Keywords: blockchain attacks; attack techniques; 51% attack; vulnerability

1. Introduction

Blockchain is an immutable Distributed Ledger Technology (DLT) that is constructed upon a peer-to-peer (P2P) network forming the data explicit to its participants in real-time [1]. The blockchain is a tamper-proof ledger technology that has the capability to store data globally. The ledger is maintained by the nodes across the network while changes to the ledger need to be agreed by the nodes prior to being added to the ledger. In bitcoin blockchain, a set of transactions of an allocated size-limit makes up a block. Each block is linked to the previous block through a cryptographic hash function, which is a method to enhance security [2].

Private and public blockchains are the common types of blockchain that are being leveraged by various entities. The verification process of both types of blockchain differs in many ways. Mostly, in private blockchains, limited numbers of selected users may be involved in the verification

process, whereas, in public blockchain, anyone can participate. Despite being one of the ingenious inventions of the current era [3,4], the robustness of blockchain is slowly dimmed by various new-age security attacks [5,6]. Although researchers and security specialists surmised many of the attacks implausible anticipating to cause no harm to the network, attackers have proved such assumptions acutely wrong by carrying out attacks exploiting weaknesses in consensus protocols.

As of 5 August 2020, there are over 6088 cryptocurrencies, whereas new cryptocurrencies are being introduced very constantly [7]. Most of the new and existing cryptocurrencies have inherited Proof of Work (PoW) consensus rules to drive their network activities. However, utilizing the same consensus protocol does not ensure the same level of security to individual cryptocurrencies. Many new cryptocurrency network remain vulnerable due to the false estimation of security rules in place. PoW protocol follows a set of rules which occur at the consensus layer [8]. Nodes select transactions according to their requirements and start solving the mathematical puzzle. The major challenge is that the protocol allows the network nodes to always accept a chain that is longer than the current chain [9]. Another drawback of the current bitcoin blockchain is its scalability problem. Each block can hold transactions up to 1 MB; hence, miners tend to include transactions with smaller size but higher incentives [10]. This creates serious issues among participants wanting to send large-sized transactions of low amount. Their transaction remains in the mempool for an extensive period before being picked by miners when offered lower fees [11]. Similarly, confirmed transactions within a block require to wait for a certain number of mined blocks added to the chain before they can be considered as fully confirmed [12].

Random attackers have endeavored various techniques to exploit blockchain, which include exploiting the P2P network, smart contracts, wallets, or the consensus protocol [13]. Amongst those, exploiting consensus protocol vulnerabilities has been quite frequent in recent times by executing techniques, such as 51% attack, Selfish mining, etc. In most cases, the level of complexity of such attacks varies based on the attacker's ability to attain the degree of hashing power. Easily achievable hashing has often been the reason for the exploitation and can seriously jeopardize the security of a cryptocurrency. Similarly, the cryptocurrency software is updated conveniently to enhance new features, as well as to cope with the security vulnerability. Undetected software bugs can be a threat to the security of any cryptocurrency. Recent bugs in the `bitcoin core` endorsed that a vulnerability remained fully undetected that could lead to a catastrophic scenario resulting in all bitcoins be drained [14]. The initial estimated attack cost was around $80,000, but, thankfully, the bug was detected in time allowing developers to fix the issue privately [15].

In this paper, we emphasize the majority hash rate challenges and PoW weaknesses that result in various exploitation, such as 51% attack, `n` confirmation attack, selfish mining, etc. We also introduce a sorting method to mitigate transaction processing issues with large-sized transactions. Due to the longest chain rule in the current PoW, a fraudulent longer chain always remains valid canceling the genuine chain of blocks. The impact of such action is fatal. Besides costing millions of dollars, it severely affects the value of a cryptocurrency itself. Furthermore, it creates disbelief amongst the miners to be part of the mining process, also discourages users from adopting that particular cryptocurrency. To solve these problems, we introduce Proof of Adjourn (PoAj), a novel technique to mitigate various attacks. Our proposed method does not recognize the longest chain to verify the genuineness of the chain; instead, it imposes an adjourn period to regulate block verification. Although network participants with ample hashing power may get an advantage through the mining process, broadcasting more than 1 block will disqualify their block to be included in the chain by refraining with mining activities for a certain period. Hence, the security of our proposed method resides removing the possibility of reversion of blocks.

PoAj confirms a transaction after just 1 confirmation, scrapping the 6 confirmation waiting time introduced in PoW; thus, it has a much faster transaction confirmation rate comparing to many exiting consensus protocols. It also introduces a unique approach that triggers when there is more than 1 block

broadcasted within a set time-frame. The introduced approach is unique and, to our best knowledge, the first approach to solve the issue. It also solves a significant issue with large-sized transactions.

The major contributions of this paper are:

1. We define the current challenges related to the majority hash rate problem and also indicate the dreadful effects of such attacks.
2. We analyze 5 major protection techniques that aim to defend major blockchain attacks. Our analysis reveals the weaknesses of the protection techniques, indicating that the threats still exist.
3. We propose Proof of Adjourn (PoAj), a novel approach to mitigate security issues introduced by the majority hash rate and by inherited weaknesses of the consensus protocol itself.
4. We also solve the issues related to transaction waiting time of large-sized low-fees transactions. The solution has also been incorporated into the proposed Proof of Adjourn (PoAj).

The rest of the paper is organized as follows.

The background Section 2, provides full information about blockchain and cryptocurrencies, the significance of the consensus protocol, security strengths, etc. In Section 3, we discuss the security aspects of blockchain technology, focusing on both the strengths and weaknesses. In Section 4, we discuss five different attacks of blockchain. We start the section elaborating significant attacks that primarily occur in PoW based blockchain and also include a small discussion about future challenges likely to affect the bitcoin blockchain. Section 5 discusses the 5 most recent protection techniques. In this section, we also identify their limitations. In Section 6, we propose Proof of Adjourn (PoAj), a novel consensus protocol that overcomes significant limitations of PoW protocol and provides strong protection against blockchain attacks. In Section 7, we assess the effectiveness of the proposed method by showing the attacks it is able to mitigate, and, finally, Section 8 is the concluding section that discusses the outcome of the overall work.

2. Background

This section reviews some of the essential aspects of blockchain technology. In particular, we emphasize discussing consensus protocols, decentralization, the relevance between cryptocurrencies and blockchain, literature related to blockchain transactions, etc.

2.1. Blockchain Technology

Blockchain is a decentralized, distributed platform where cryptocurrencies are classified as one of its class [1]. Blockchain is the core technology where the cryptocurrencies are an important part of the ecosystem. Besides cryptocurrencies, blockchain can also be utilized in smart contract applications, a few areas of which are the banking sector, healthcare, property agencies, and supply chain. Many organizations have also adopted the blockchain to secure their confidential data and endorse the identity of investors [16].

The bitcoin protocol is built on the public blockchain allowing anyone to join the network, whereas various organizations take advantage of the private or permissioned blockchain allowing only authorized parties to join the private network [17]. Blockchain is often referred to as distributed ledger technology (DLT), comprising unique features that help reduce risks, distinguishing fraudulent activities, and also bringing transparency among the network nodes. A node can be part of the network through any device keeping all copies of the digital ledger.

2.2. Decentralization

Blockchain is based on a decentralization method where the nodes do not rely on a central entity [18]. The decentralization can be described in various ways [19]; in simple terms, blockchain can be classified as politically decentralized as it is not controlled by a single authority, and it is also architectural decentralized since failure to certain nodes does not affect the network flow; however, in a

logical view, they are centralized as the whole system follows the same approach as a single computer. The decentralization is important because of three major components. First, fault tolerance enhances the blockchain to depend on various entities in the network. Second, it is attack resistance as the cost of an attack is often too expensive requiring adversaries to target various components of the network to be successful. Finally, it is collusion resistance restricting participants to benefit at the cost of others.

2.3. Cryptocurrencies

Cryptocurrencies are an electronic cash system that exists electronically [20]. Unlike fiat currencies, cryptocurrencies are not monitored by any central authority and utilize P2P system to carry out transfers. Bitcoin, Ethereum, Bitcoin Cash, and Litecoin are some of the major cryptocurrencies widely used by various groups of users. Low fees, global transaction facility, and fast payments, as well as fraud detection, have made the cryptocurrencies very popular and quickly embraced by various groups of users [21].

A crypto transaction may occur in various forms, and it must go through a few stages before it gets confirmed [22]. Once a transaction is initiated, it is visible in the mempool for miners to pick. Successfully mined and confirmed blocks can still be canceled. Therefore, transactions within a particular block can be considered secure when additional blocks are added in the chain.

2.4. Transaction Fees

The bitcoin miners use powerful systems to complete the mining process. The cost to maintain such computers is very costly and may incur a huge loss if the system is unable to compete with the pace of the other mining systems. Hence, transaction fees are a way to reward the miners for driving the network flow [23]. Different cryptocurrencies have distinct ways of rewarding their miners. In bitcoin blockchain, the more satoshi (the smallest unit of a bitcoin) is offered per bytes of space, the more it is prioritized by the miners; thus, the chance of mining increases.

The bitcoin wallet advises a user the approximate transaction fee prior to making a transaction. Each transaction is a file that takes up some space. The transaction fees are determined based on the inputs and outputs of any transaction contains. Hence, the transaction amount does not reflect the transaction fees, rather the fee depends on how much space a transaction takes on a particular block.

2.5. Master Nodes

A masternode is an alternative way of mining [24]. It is a full node which assists the blockchain network by hosting a live copy of the ledger. The masternode gets rewarded for its enhanced support to the network. Bitcoin and Dash are the two cryptocoins that implemented the masternode method. There are various reasons for running masternode, but one of the most important aspects is that it helps to boost the privacy of the transactions. Moreover, factors, such as permitting instant transactions and voting facilities, are also possible while leveraging the masternode approach. The profit in running a masternode may vary upon the selected cryptocoin, the protocol utilized, etc.

2.6. Consensus Protocol

The consensus protocols are one of the significant parts of a blockchain network ensuring that the network performs according to the set rules [25]. Reaching into an agreement amongst the network participants can be far from an easy task. The network must ensure that all the trust-less nodes agree to the solved work of a miner. Consensus protocol makes it easy to ensure that every participating node is abiding the protocol rules.

PoW is one of the prime consensus protocols utilized in bitcoin and other major cryptocurrencies. Besides that, Proof of stake (PoS), Delegated Proof of Stake (DPoS), Proof of Activity (PoA), and Proof of Authority (PoA) are a few of the protocols which are being used by many cryptocurrencies based on their mining criteria and other factors [26–28]. Recent research shows most of the consensus protocols remain vulnerable and the basis for many blockchain attacks [5,6].

2.7. Merkle Tree

The Merkle tree is a hashing process that is used in blockchain to generate a hash value [29]. Figure 1 shows an illustration where all transaction hashes are added up to generate a Merkle tree within a block and how blocks are connected to each other.

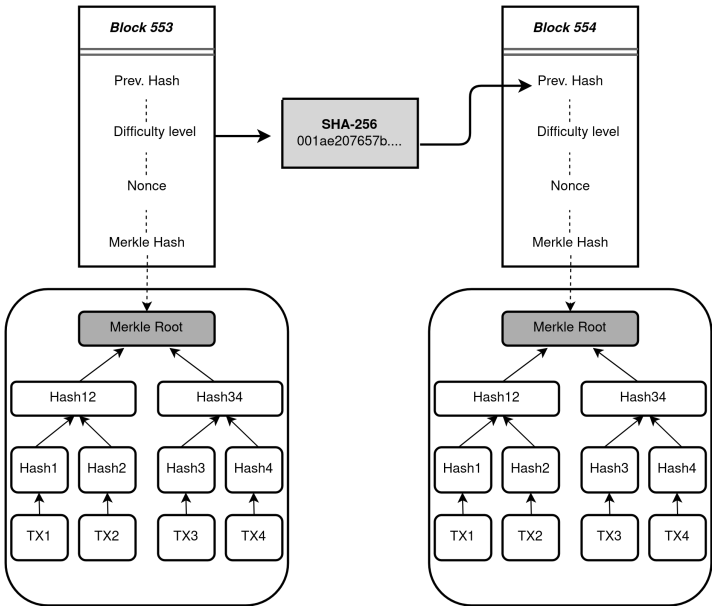

Figure 1. An illustration of Merkle root of bitcoin blockchain.

In Bitcoin blockchain, every transaction is hashed until a single hash value is obtained from all. For instance, if a bitcoin block contains 4 transactions `TX1, TX2, TX3, and TX4`, all of the 4 transactions to be hashed by SHA-256. The hash of TX1 will be merged with the hash of TX2, and then both hashes will again be merged until a single hash value is obtained. Similarly, the same rule applies for TX3 and TX4. The process continues as a tree-like structure until a single fixed-length hash is obtained which is called the Merkle root.

2.8. UTXO: Input/Output

Bitcoin and many other cryptocurrencies follow the Unspent Transaction Output (UTXO) approach to process the transactions [30,31]. Bitcoin wallet saves the record of any transactions that are to be spent in the future. Figure 2 shows that Alice has 11.5 BTC in her wallet, which she received from 4 separate sources. She requires to send 6.0 BTC to Bob for which she unlocks 3 of the transactions. Since the 3 transaction adds up 7.0 BTC, 1.0 BTC can be returned from Bob as output and added to her wallet as a separate UTXO with any previous UTXO. Alice requires to mention the fees, that are to be deducted from 1.0 BTC. For the sake of simplicity, the fees are not included in our example.

This scenario is similar to a banknote where a consumer hands-in $10.00 note for goods worth $8.00 and receives his change. The size of any transaction varies based upon the number of inputs/outputs, and transaction fees can be calculated in the following way;

```
Transaction Fees = TX(Input) - (TX(output) + Change)
```

It is the senders' discretion to offer how much transaction fees she is willing to offer. However, lower fees might leave a crypto transaction in the pool for way too long as miners are often not encouraged to mine transactions with lower fees. The main advantage of the UTXO based system is its scalability and privacy.

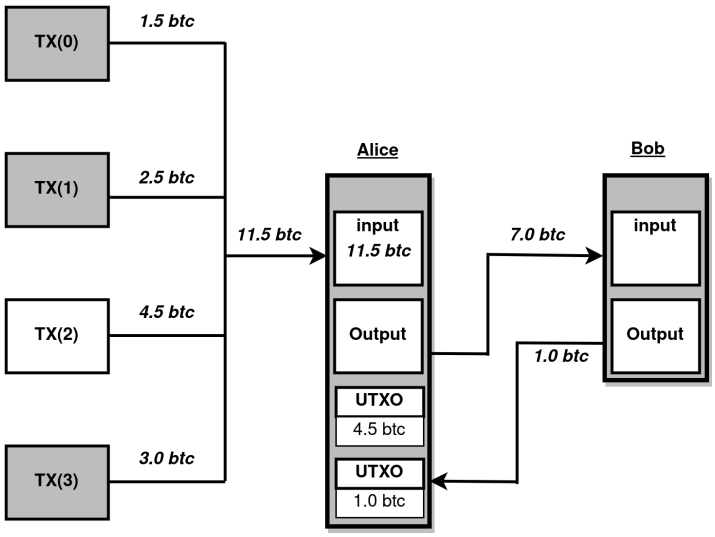

Figure 2. An example of Unspent Transaction Output (UTXO) where Alice sends 7 bitcoins to Bob.

2.9. Account-Based Model

Account-based model is another approach that works by tracking the account balance [31]. Ethereum leverages an account-based model for its digital transactions. This model works similarly as a bank account that verifies the account balance before sending funds out. Account-based model is a simple approach for smart contract developers. One of the major advantages of the ethereum's account based system is that accepts stale blocks reducing the waste of mining powers. The stale blocks are called uncle blocks. In addition, the account-based model is very much efficient as each crypto-transaction requires a single check to verify if a participant account holds enough coin to authorize a transaction.

2.10. Lightning Network

The lightning network is an extra layer of payment medium that allows users to make payments frequently [32]. This network can occur between two parties where they can transfer cryptocoin instantly. Besides instant transactions, users also do not require to pay higher fees since all transactions do not go through the mining process. This payment channel mainly occurs between parties who require to transfer funds on a frequent basis. The users are required to maintain a multi-signature wallet and both users can have access to the wallet using their private keys.

The funds remain in a shared wallet, and when both parties decide to close the payment channel then the algorithm calculates the accurate amount for each party. The final balance is then broadcast to the main bitcoin blockchain network for miners to add in their mining blocks. The scalability problem is a great challenge for the current bitcoin network. Visa executes 24,000 transactions per second, whereas the bitcoin is only able to process 7 transactions per second. Hence, the lightning network somewhat solves bitcoins scalability problem to a minimal extend when transferring funds between known parties.

3. Security Aspects

In this section, we discuss the security aspects of blockchain technology. Blockchain has solved many security challenges encouraging all levels of users to adopt the technology. It comprises unique security features that distinguish it from other secured frameworks. Decentralization, cryptographic hash functions, and immutable ledger, as well as solving the most difficult challenging part, such as Byzantine fault tolerance (BFT) [33], has endorsed blockchain as a secure technology. However, blockchain is not a solution to all security issues, and there are vulnerabilities exist that need to be addressed, as well.

This section aims to provide a basic understanding of security features and flaws of the blockchain technology.

3.1. Application Flaws

Blockchain nodes use the same client software to manage network activities. Simple bugs in the software can be proven catastrophic costing millions of dollars. A software update is a process to fix bugs and reduce attacking opportunities. The *bitcoin core* gets updated to tackle flaws and implement robust features. In most recent, a severe vulnerability was discovered in bitcoin, and if it remained undetected, the impact of the found vulnerability could be catastrophic enabling attackers to crash the whole crypto-currency [15]. Similarly, many users are unaware of the genuine exchanges or wallet applications. Fake exchanges and wallets have been a common bait to steal cryptocurrency [34]. Electrum, a bitcoin wallet has been compromised to lose the worth of $937,000. Attackers created a fake version of the wallet encouraging users to provide password detail.

3.2. Double Spending

The double spending is a method to spend the same digital asset more than once. It is usually executed through various exploitation techniques. Adversaries initiate 2 transactions from the same version of cryptocoin, one of which is a valid transaction but intend to benefit from both as the other transaction gets canceled [35]. Double-spending is one of the most crucial attacks to the cryptocurrencies because it exploits a weakness in the consensus protocol itself. In 51% attack, one confirmation attack are the types of attacks used to double-spend the same crypto-coin [36]. Attackers can execute double-spend into a crypto-coin in various ways, for example, by provoking a seller to release goods without any confirmation or executing different attack techniques while in possession of plenty of hashing power.

3.3. Blockchain Centralization

Although being labeled as decentralized, many components of the blockchain ecosystem is fully centralized. For instance, about 70% of the mining pools of bitcoin blockchain are based on a single location [19]. Mining concentration on a few mining pools is a huge security risk that attackers could abuse; for example, it reduces the effort necessary to launch denial of service attacks since attackers require to control fewer physical devices to success.

In addition to that, a huge number of cryptocurrency users utilize centralized cryptocurrency exchanges [37]. The centralized exchanges work in a similar way as a bank that is owned by a single entity. Although most of the centralized exchanges are safe for crypto-transactions, there still a risk involves for being the focal point. Moreover, exchanges can be vanished at any point closing down the business. A report suggests that 14 crypto-exchanges were exploited between 2017 and 2018 with an estimated loss of $882 million [38].

3.4. Byzantine Fault Tolerance (BFT)

Byzantine fault Tolerance (BFT) is one of the crucial parts of blockchain as it enhances the ability of a node to continue performing as normal when a part of the network is obstructed by attackers [39]. It is the capacity of the blockchain network to agree on the verification of the current state of the transactions on a regular basis. BFT is named after a solution of a problem which is known as "Byzantine Generals' Problem". The scenario involves a group of Byzantine generals who surround an attacking point aiming to conduct an attack with their army. For the attack to be successful, all the surrounded army must act at the same time. The attack to be precise, the information regarding the attack to be passed from one to another. However, having a traitor general, who passes false information to others, the attack becomes unsuccessful as the whole army fails to act at the same time. In the blockchain, while a few nodes pass malicious information can not harm to the network as all active nodes require to agree on a single state discarding malicious activity.

The BFT feature in cryptocurrency ensures that all nodes reach a consensus and not affected when there is an existence of malicious node to misguide other nodes in the network [33]. BFT is an essential part of the blockchain and also works as a safeguard to defend against malicious nodes' harmful behavior.

3.5. Cryptographic Hash

Blockchain utilizes cryptographically secure hash functions to ensure data integrity and security of the overall process. The hashing process generates a value of the string using mathematical functions [40]. It is a one-way process that does not permit the hash function to reverse back to its previous state. SHA-256, MD5, and Keccak-256 are some of the hash functions used by major currencies. Cryptocoin adopts distinct hash functions due to its operational requirement. Although, bitcoin and many other cryptocurrencies have adopted SHA-256; SCRYPT is currently the choice for newly generated cryptocoins for its speedy feature [41].

Public key cryptography is another aspect in the blockchain which is utilized to validate data and authenticate users through digital signatures [42]. The authentication is ensured by combining both the users' public and private key through the Public Key Infrastructure (PKI) method. The public key is released to the general public to recognize a user's identity and can be used to perform digital transfers. Mathematical functionalities generate both the private and public keys enabling to encrypt and decrypt the information sent.

4. The Problem: Cryptocurrency Attacks

The main strength of blockchain technology is the verification of data through a distributed approach. Besides that, the decentralized and distributed network infrastructure helps to prevent many centralized attack techniques. However, Verge (XVG) [43], Ethereum Classic (ETC) [44], etc., are some of the coins that have been severely affected by 51% attack [5]. Similarly, well-established coins, such as Bitcoin Gold (BTG), has also suffered twice from the same attack technique [45], whereas most other cryptocurrencies are also vulnerable due to the weaknesses in the consensus protocol.

In this section, we present five cryptocurrency attacks that seriously jeopardize cryptocurrencies that are mainly based on the PoW consensus protocol. We also discuss future security issues that are very likely to occur in the near future due to the intrinsic weakness in the PoW consensus protocol.

4.1. 51% Attack

The 51% attack is an attacking technique executed by attackers while comprising at least 51% of the total hashing of a particular cryptocurrency [46]. Figure 3 shows a scenario where the attacker executes double-spending through a 51% attack. The scenario also explains a selfish mining technique. Block 2058 is a genuine block that is reversed when a selfish miner produces his block 2058 and 2059. The selfish miner's chain becomes the main chain as the network starts building their work on it; in this case, block 2060 is added. However, an attacker with 51% hashing power produces an even longer chain from block 2059 to block `n`, which again makes the network follow the attacker's chain, canceling all transactions from block 2059 to block 2060.

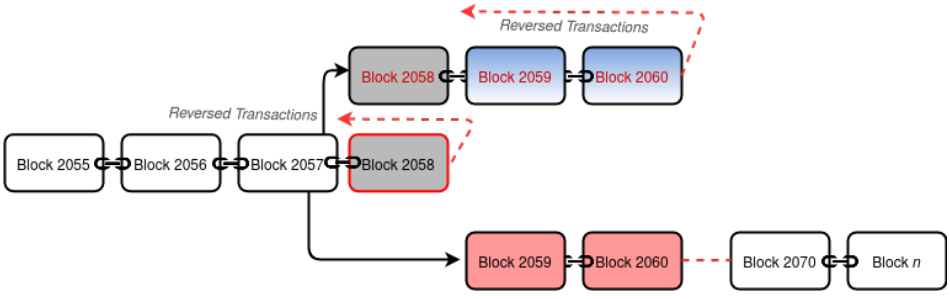

Figure 3. A 51% attack scenario where the attacker executes double-spending.

Cryptocurrencies with high hashing power are considered more secure as it costs significantly high amount for attackers to initiate the attack [47]. Hence, attackers mainly target cryptocoins with low hashing power. A successful 51% attack may allow attackers to cancel confirmed transactions, double-spend the same cryptocurrency, control the price of the coin, or fully crash the whole blockchain network.

Although the attacking cost is immensely high, the profit margin is also very high that encourages attackers more compared to other blockchain attacks. The 51% attack requires an adversary to develop its chain in private. Due to the longest chain rule, attackers can successfully exploit the vulnerability when they are able to build a chain that is longer than the current chain [9,48]. The attackers generated chain overlaps the main chain compelling the network to follow their chain. The attacking pattern differs based on the adopted consensus protocol.

4.2. Selfish Mining

The selfish mining is a majority hash rate attack occurs when a miner or mining pool dominates with a large amount of hashing ability [49,50]. Currently, a few bitcoin mining pools comprise enough hashing power to execute selfish mining [51]. The main idea of this attack technique is to keep blocks in secret from the public chain and continue mining on the secret chain.

Selfish mining is a way to waste the rival miners' computations. The selfish miner always intends to remain 1 block ahead. By revealing the longer chain, the selfish miner receives rewards for his current block and also any block of its rival that has been discarded. Selfish mining can be accomplished with approximately 25% of the total network hashing. If selfish mining occurs at a frequent pace, then independent nodes likely to join the selfish miner's pool to increase their profits, and this can give the corrupt pool more control over the network by boosting up their hashing power.

4.3. Miner Bribe Attack

Miner Bribe attack is another attacking scenario where an adversary deceives a purchasing activity. Assuming a scenario where the consumer receives his products instantly without the transactions being confirmed [52], for instance, vending machine purchases. Once the transaction is being processed, the adversary acts fast to sign the transaction to spend the same coins back on his wallet. The attacker offers higher fees for his second transaction to ramp up the chances to be mined first. The second malicious transaction will have a higher chance to be picked for mining as miners tend to choose transactions with higher fees. An experiment over Miner Bribe Attack shows that over 4220 attempts were made for such attacks where the success rate resulted in 88%. However, the time-delay between transactions is a crucial factor as that success rate was achieved with a minimum delay of 0.00–2.05 s.

4.4. Zero Confirmation Attack

The Zero confirmation attack is another technique exploited in a similar way as the Miner bribe attack. A Zero confirmation attack can be executed to double-spend a cryptocurrency [53]. It is exploited by persuading a merchant where goods are received on an instant basis, for instance, ATM transactions, online transactions, etc. [54]. It requires an adversary to generate two outputs `TX1 and TX2` from `TX0`. The attacker's main aim is to gain a merchant's trust and persuade them to believe that `TX1` is a legit transaction so that the products are released. The merchant releases goods while the transaction is yet to be confirmed in the block, the attacker gets `TX2` added discarding `TX1`.

4.5. One Confirmation Attack

One confirmation attack comprises a similar scenario as zero confirmation attack [55]. The attack can be conducted in many different ways for successful exploitation. Consider a scenario where merchants tend to release their goods after one block confirmation. Attackers having their transactions in a stale block will have the opportunity to perform double-spending. While 2 or more blocks are at the same height, the majority miners follow the block that is seen first to start building with the next

block. A chain with the highest work is always followed; hence, confirmed transactions added to the orphaned block gets rejected and sent back to the mempool for re-mining, allowing the attacker to receive his spent coins back that were used to pay for the goods.

Figure 4 shows a scenario where an attacker initiates double-spending through one confirmation attack. At block height 2058, 2 blocks are broadcast where both are legit. However, the block that is seen by the majority of the nodes is followed by discarding the orphan block at the same height, hence reversing all of its transactions.

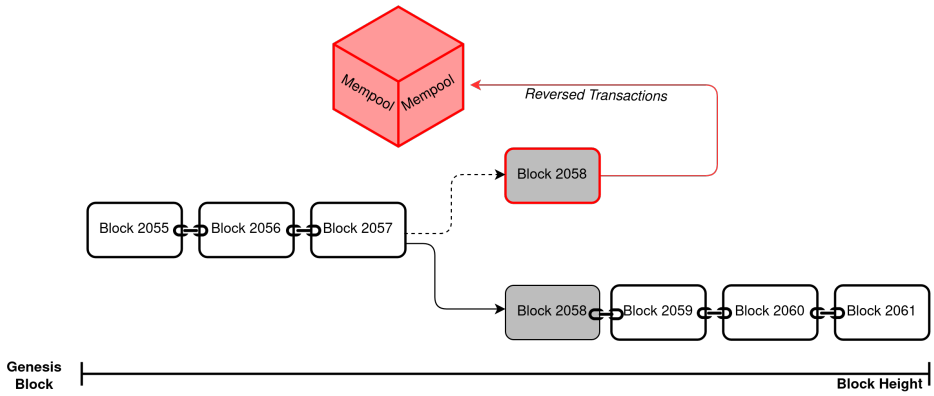

Figure 4. Example of 1 confirmation attack while a stale block triggers in the blockchain.

4.6. Future Problems

The blockchain is relatively a new technology with a solution of various security issues. Many attacking techniques were presumed impractical; however, they were executed in a frequent manner showing that any assumptions made were wrong. In a similar way, the bitcoin blockchain comprises weaknesses that may be challenging at a later stage.

There are many countries where cryptocurrency tradings are fully illegal [56]. Many governments are also in fear that the cryptocurrencies can be used by criminals for illicit activities as the currency is not regulated. Since the immense capital is one of the main barriers to execute a successful attack, a government body can fund to stop an entire blockchain network to fulfill their national interest.

About 70% of the Bitcoin mining pools are based on a centralized location [51]. Cheap computing power and low hardware, as well as electricity cost, are some of the main reasons for miners to set up mining hubs in particular locations. In recent times, the National Development Reform Commission, China's top economic planning body proposed to ban cryptocurrency miners [57]. If banned, such events may be catastrophic to many cryptocurrencies including bitcoin itself as the network hash rate will decline sharply making the entire network fully exploitable to many attacks. The execution cost of several attacks might also come down near to nothing due to the decline in the network hash.

As of 3 August 2020, the total market capitalization of bitcoin is 117.81 billion US$ [58]. Due to the centralization mining approach, a 2–3 mining pool can easily make up about 51% of the total network hashing. Mining pools can also join together to perform malicious acts to harm the entire bitcoin network costing billions to the cryptocurrency users. Similarly, the application development team that is involved in updating the cryptocurrency software, or the research community responsible for making significant proposals may involve in fraudulent activities to affect the entire network [19]. In addition to that, the mining hardware is also produced by only a few companies. Implementing hardware trojans, malicious kits, or hardware faults is also possible and can hugely impact the overall flow of any cryptocurrency.

5. Current Protection Techniques and Limitation

In this section, we discuss five major protection techniques and their limitations. Our analysis indicates that although somewhat protective, the protection techniques fail to protect against the major attack presented in Section 4.

5.1. A Penalty System for Delayed Block Submission

A penalty system for delayed block submission is a security proposal by Horizen [59]. The proposal is based on modifying the PoW consensus and impose a penalty to the attacker to ramp up the attacking cost. The degree of penalty to be determined based on the time the attacker's block is hidden from the network. Upon detecting a longer fork, the entire network will be notified about the event and will be barred in performing any transactions until the delay period is lifted.

Unfortunately, the penalty system for delayed block submission comprises a few limitations. In order to beat the six block confirmation , an adversary will be introduced to a delay of 21 blocks. Having successfully mined the penalty blocks in a sequence the delay will be lifted and the mined blocks to be included in the normal chain. According to Rosenfeld, on any occasion, while an adversary owns 51% of the hashing power, he will always succeed regardless of the enforced delay [48]. Moreover, transactions added to the delay blocks might not be confirmed until the delay is lifted. Hence, the whole process will severely impact the regular flow of the network.

5.2. Delayed Proof of Work (dPoW)

Delayed proof of work (dPoW) is a security solution by Komodo implemented for UTXO based cryptocurrencies. The security technique is already implemented in a few blockchains to defend against double-spending attacks [60]. The dPoW does not recognize the longest chain rule; hence, attackers intending to develop a chain in private cannot gain an advantage to double spend. dPoW elects 64 special nodes each year to process the required task. The nodes involved in acquiring information from Komodo to save it in the bitcoin blockchain. The strengthened security approach requires the attacker to rewrite the komodo chain and bitcoin checkpoints. Moreover, the attacker also needs to influence the majority of the notary network.

The drawback of dPoW is that it requires a regular fee to leverage the service. It also has a significant waiting time for the notarization to accomplish. The extensive notarization time does not fully protect cryptocurrencies which have only a few seconds of confirmation time, giving attackers enough time to execute a 51% attack. Moreover, the special nodes can be a centric point to attackers.

5.3. Pirlguard

PilGuard is another security approach that modifies the consensus rule to defend against a 51% attack [61]. It is primarily built for Ethash. Its protection approach is similar to Horizen's "The Penalty System for Delayed Block Submission". When the network detects privately mined longer blocks, it abandons the peer instantly by penalizing to mine x number of blocks. The penalty is calculated based on the total blocks mined in secret. Pilguard utilizes notary contracts, managed by the master nodes. Master nodes are responsible for notarizing the blockchain and penalizing malicious actors by retrieving the legit consensus on the Pirl blockchain.

As discussed earlier, a penalty is not an ultimate solution to defend against the attack because of attackers with 51% hashing are likely to beat the penalty. Moreover, providing authority to master nodes makes them a focal point to the attackers which is certainly a security issue.

5.4. ChainLocks

ChainLocks is another security approach that is developed to secure DASH. It has resulted from the implementation of long living masternode quorums (LLMQs) to mitigate the 51% attack [62]. ChainLocks introduces a network-wide vote process that induces a "first-seen" policy. For each

particular block, an LLMQ of a large number of master nodes is approved. Every network participants need to sign the notice block to extend the active chain. While 60% or more network participants verify a block, they generate a P2P message (CLSIG) to notify every other node about the event. ChainLocks follows one confirmation transaction rule, forbids a confirmed block to reverse back since a signed block can not be acknowledged at a later time.

The major disadvantage of ChainLocks is that it is based on only one single currency, Dash. Besides the low network hashing of Dash, the master node approach makes this a weak security approach [63]. Nicehash is a hash renting facility which rents out hashing power [64]. Low hashing cryptocoins are at great risk as giving attackers the opportunity to fulfill their hashing shortage by renting more hashing power.

5.5. Merged Mining

Merged mining is not a security technique but an approach that allows multiple cryptocurrencies to be merged to mine at the same time [65]. Cryptocurrencies with low hashing power can benefit from this approach to enhance security. The process allows to increase the hashing power by bootstrapping on the other currency that comprises higher hashing power. While cryptocurrencies are leveraging merged mining, both blockchain networks can run in a sequence. The blockchains are classified as a parent and auxiliary blockchain. It gives miners an advantage to mine more than a block simultaneously.

Although merged mining boosts the security, the process is quite complicated and often neglected by miners. Cryptocurrencies that are taking advantage of this approach must be on the same consensus protocol and mining algorithms [66]. All the cryptocurrencies are not supported by merged mining; moreover, if two low hashing cryptocoins merge together, then they might not fully be benefited from this approach while the merged hashing is still achievable by attackers.

6. Proposed Solution: Proof of Adjourn (PoAj)

In this section, we introduce Proof of Adjourn (PoAj), a novel approach to mitigate major blockchain attacks, and the transaction processing delay issue with large-sized transactions on UTXO based coins.

The key idea of the proposed method is that it adjourns the network nodes from all activities by introducing an Adjourn Period (AP). Any broadcast block will be considered as Initial Block (IB), and will not be confirmed until the AP is finished. Our novel design divides the AP into 2 phases to perform two distinct tasks mitigating significant PoW attacks. The first phase performs verification checks to n number of IB's which last up-to a pre-set time. The second phase only triggers based on the outcome of the first phase. Once the AP is over, the newly verified and selected block gets added to the blockchain, allowing miners to restart with the mining process again.

In any case, an IB fails to meet the condition checks at Phase 1, it gets discarded with an imposed penalty by setting off the network for restarting the mining process. Unlike PoW, PoAj does not recognize the longest chain rule, rather Phase 1 is the prime phase that verifies whether a block is a legit block. Figure 5 illustrates an overview of the working phases of the novel security approach.

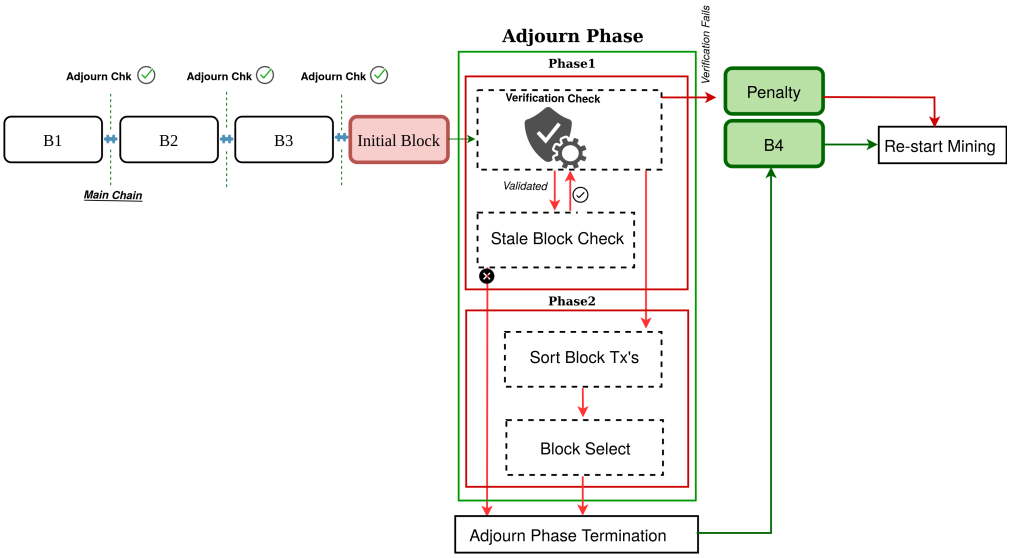

Figure 5. Proof of Adjourn (PoAj) design.

6.1. The Approach

The total Adjourn Period (AP) is any period that includes expected Block Verification time (eBVT) and Block Sorting Time (BST). It takes only a few seconds to broadcast a block over the network [67]. The eBVT may vary and can be set based on the particular network structure where the time takes of majority of network nodes to propagate to each other. This enables major network nodes to enter the AP when they have successfully mined a block. The Block Sorting Time (BST) is only executed if the Initial Block (IB) is more than 1. We define Maximum Waiting Time (MWT) as the total time which includes Block Generation Time (BGT) and expected Block Verification time (eBVT). Hence, at anytime a node does not get notified about the IB within the MWT, then it should halt all its activities and wait for acknowledgments from its peer nodes.

Adjourn Period (AP) = expected Block Verification Time (eBVT) + Block Sorting Time (BST)
Max. Waiting Time (MWT) = Block Generation Time (BGT) + expected Block Verification Time (eBVT)

Assuming a miner be the first to solve the mathematical puzzle and broadcasts his work to the network, the working path of PoAj goes as follows; As soon as a block is broadcast, any node that acknowledges the outcome enters the AP. PoAj consists of 2 phases where the first phase executes certain conditions to determine the legitimacy of the IB. When the eBVT is persistent in nodes, the total period remains valid based on the point in time of the first IB, any number of IB can enter the AP and get verified. Any IB that has completed the verification process remains in the phase until the pre-set eBVT is over. If there is more than one IB broadcast within the eBVT period, both blocks go through the verification process.

Once the eBVT ends, the total number of verified IB is counted. If more than 1 IB is verified as legit, it sets off the next phase by executing a sorting approach to sort each block based on their large-sized transactions. The sorted large-sized transactions are then compared to each of the same height block transactions. The block that has the most number of large-sized transactions is selected as a confirmed block. If two or more blocks have same-sized transactions at the same height, then both get counted to receive a point. Since each particular blocks will have a different number of transaction; therefore, the comparison count will be based on the least number of transactions any block consists.

Figure 6 shows that Block A consists of 4 transactions, whereas Block B and C consists of 5 and 6 transactions. Block A having the least number of transactions, the comparison will occur 4 times. The first sorted transaction of Block A is 85 bytes that are higher than the transaction of Block B and C

giving it 2 points. However, the rest of the transaction's size is lower than the other blocks' transactions. Hence, Block A only receives 2 points for one large-sized transaction.

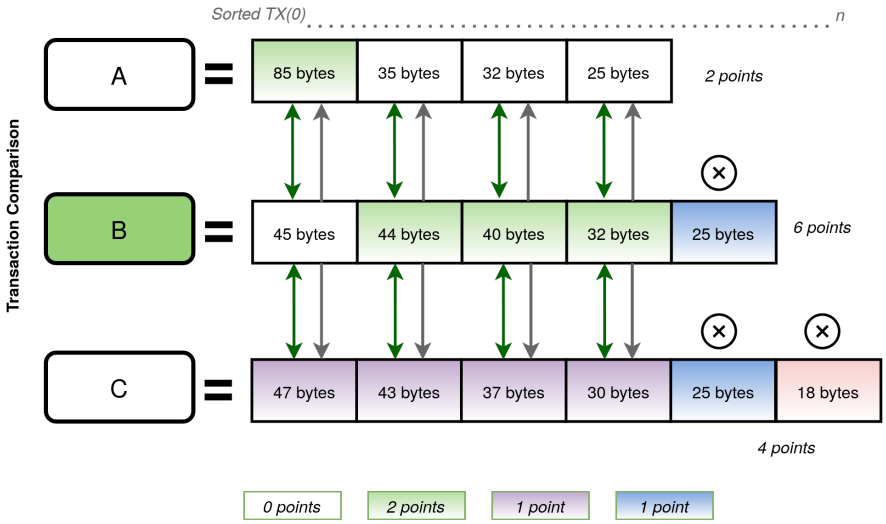

Figure 6. Sorting transactions to determine a block with most number of large-sized transactions.

It is important to note that the sorting approach encourages miners to pick transactions based on their size, not based on fees. Besides selecting the confirmed block, PoAj mitigates the problem of large-sized transactions being in the mempool for a longer period. Upon finishing the Phase 2, the selected block gets confirmed in the main chain by changing the status to `Confirmed Block` from Initial Block (IB). The single confirmation endorses IB as a legit block without needing to wait for 6 confirmation. Both phases of the AP period are executed in every node of the network and always results in the same outcome. If one or more IB's fail to satisfy the verification criteria, they will be discarded with a penalty over their node, and the network restarts the mining process.

6.2. The Implementation

We have implemented a proof of concept of the proposed Proof of adjourn (PoAj) consensus protocol. For the sake of readability, we chose python since this language has already defined methods that are simple and reduce the final code. The code contains no optimization intentionally to better show the approach and to facilitate the explanation of the PoAj steps.

Listing 1 shows the steps of verifying Initial Blocks (IB). An IB needs to go through certain verification checks, for instance, whether the Current block height has incremented by only 1 at the current stage, the saved hash matches with the previous hash value, and whether the Block Generation Time (BGT) is less than 300 s.

Listing 1. Verification checks of Initial Blocks (IB) within the pre-set 40 s time.

```
# Apply Penalty
def apply_penalty():
    # 1000 Seconds Penalty
    time.sleep(1000)

# Verify Blocks
def verify_blocks():
   global~totalBlocks

   current = time.time()
   for blk in blocksList:
       if CurBlockHeight != PrevBlockHeight+1:
           continue
       if SavedHashValue != PrevHashValue:
           continue
       if BlockGenerationTime < 300s:
           continue

      # Increment verified blocks
       totalBlocks += 1

   while (time.time()-current) < 40:
       time.sleep(1)

   return~0
```

It should be noted that the BGT, an expected block generation time, can be determined based on the difficulty level set by the cryptocurrency, with additional time added, ensuring that a block was not hidden for a longer time and broadcast on an instant basis. The eBVT is an assumed time, giving maximum nodes to propagate to each other with additional time added so that any orphaned blocks can also be included as IB. In Listing 2, we count the total number of IB to determine whether we enter phase 2. Assuming the total number of verified blocks is more than 1, then we need to pick the best block among them.

We have implemented a sorting approach to sort each transaction of each verified blocks based on their transaction size. Once sorted, the algorithm compares each transaction of a block to the same height transactions of the other blocks. The block that has more number of large-sized transactions, gets confirmed. Figure 6 shows an illustration where three IB's have passed the verification process but one block to be selected as a confirmed block for having the maximum number of large-sized transactions.

The transactions of each block were sorted and then compared to each other. In this case, Block B received highest points for the highest number of large-sized transactions after comparing to Block A and C. The miners are penalized when all fail to meet the conditions, by excluding them from any network activities up to n number of blocks; for the sake of simplicity we have imposed 1000 s penalty to the malicious node. Furthermore, the sorting process will not be necessary as the network will reinstate the mining.

Listing 2. Sorting IB and comparing large-sized transactions to determine the confirmed block.

```
# Return the highest block
def run_proof_of_adjourn():
    global maxPoints, totalBlocks
    sortedBlocksLst = []

    # Verification conditions check
    if verify_blocks() != 0:
        return~VER_ERROR

    # Return when there is only 1 block
    if totalBlocks == 1:
        return blocksList[0]

    # Sort Transactions
    for blk in blocksList:
        sortBlk = list(blk)
        sortBlk.sort(reverse=True)
        sortedBlocksLst.append(sortBlk)

   # Determine the lowest number of transactions
    min = len(sortedBlocksLst[0])

    # Get the Minimum
    for curBlk in sortedBlocksLst[1:]:
        num = len(curBlk)
        if num < min:
            min = num

    # Calculate the number of Large-sized transactions
    for curBlk in sortedBlocksLst:
        points = 0
        for tmpBlk in sortedBlocksLst:

    #  block comparation
          if curBlk == tmpBlk:
               continue
          for i in range(min):
              if curBlk[i] >= tmpBlk[i]:
                  points += 1

        # Highest Points Check
        if points >= maxPoints:
            maxPoints = points
            highestBlock = curBlk

    # Return the highest block
    return highestBlock
```

7. Evaluation

In this section, we evaluate the effectiveness of PoAj against the 51% attack, n confirmation attack, Selfish mining and also large-sized transaction issues. The evaluation demonstrates that PoAj mitigates the existing weaknesses.

7.1. 51% Attack

We assume a scenario where an attacker comprises enough hashing power to execute a 51% attack. Figure 7 shows that mining pool X and Y solves the mathematical work and broadcast their work to

the network at the same time. An attacker has also mined his chain privately that is longer than the main chain, and broadcasts to the network. According to PoW's longest chain concept, the attacker's chain is the chain to be adopted by the network nodes.

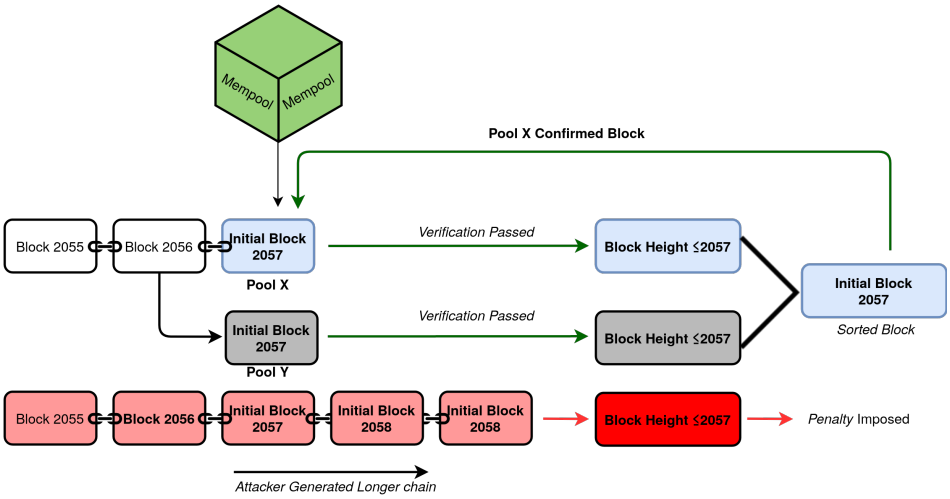

Figure 7. PoAj stopping the 51% attack.

However, PoAj applies its unique approach to deal with this problem. PoAj performs a sequence of verification checks to all the 3 solved blocks. The adjourn phase starts by checking certain conditions discussed in Section 6.2. The attackers produced chain fails to pass the verification since the bock height is higher than the expected value. PoAj immediately imposes a penalty to the attacker's node for n number of blocks or a set duration barring him from all network activities. If all the 3 blocks failed to satisfy the conditions, then the mining process restarts imposing a penalty to all 3 nodes that produced the blocks.

Although, blocks produced by mining pool X and Y pass the verification checks but yet to be confirmed until it is determined which of its miners focused on adding the large-sized transactions in their block. Figure 7 shows that after executing the sorting and comparison method, the block generated by pool X is selected as a confirmed block. The selected block immediately gets added to the main chain as a confirmed block to restart the mining process.

7.2. Transaction Confirmation Delay

The average block generation time of bitcoin blockchain is 10 min. In most cases, in the bitcoin blockchain a transaction is considered confirmed after 6 confirmation waiting time, while additional confirmations strengthen the security.

Bitcoin blockchain has a problem that results in large-sized transactions, with lower fees, to be held in the mempool for a longer period. This is because miners tend to include lower-sized transactions so that they could fit many transactions within the limited block size and get more rewards. Once large-sized lower fees transactions get added to a block after an immense waiting time, the participants still require to wait for at least 6 confirmation time to consider their transaction secure. Besides that, the current PoW consensus rules do not guarantee any specific time for a transaction to be included in the block. The transactions are not picked by order; hence, a transaction may remain in the mempool for a few days or more.

The proposed PoAj solves this problem by its novel sorting approach. Figure 8 shows that 3 blocks entered the sorting period. Block C picked its transactions according to the higher fees offered by users to speed up their transactions. Furthermore, Block C also picked the smallest-sized transactions so that it could fit the maximum number of transactions to boost its profit. However, Miners of Block A and B were encouraged to pick their transactions based on the PoAj block selection criteria. Once the novel sorting and comparison approach is applied, Block B wins the race among 3 blocks for including the

maximum large-sized transaction. It should be noted that the transaction fees do not reflect the PoAj block selection process.

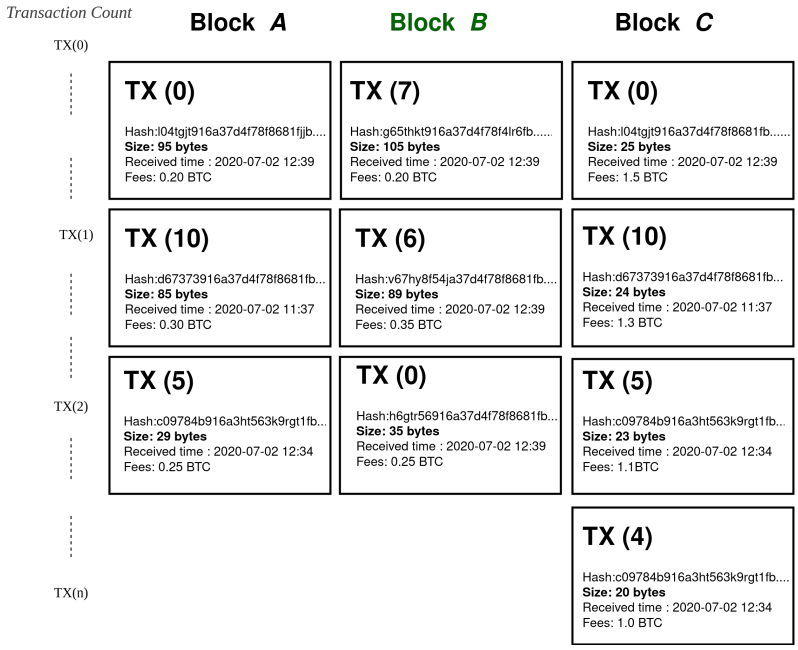

Figure 8. An example where 3 blocks are compared. Block B wins over A and C for having large-sized transactions.

7.3. N Confirmation Attack

The Zero confirmation, One confirmation, and the Miner bribe attack is an analogous attacking technique but exploited in a different way. Hence, we are defining all the attacks as `n confirmation attack` for the sake of simplicity. The main similarity among those attacking techniques is that attackers leverage the extensive block confirmation time to exploit the network. Since the PoW consensus does not process transactions in order, a transaction can take any amount of time to be confirmed. Such a weak approach is the main cause to result in these attacking methods. The long waiting time has let attackers take advantage of the situation where a merchant requires to release goods instantly.

PoAj mitigates the problems with its 1 confirmation technique where a single confirmation is final confirmation. Figure 9 shows 2 scenarios, where the confirmed transactions of block 2056 require to wait until block 2062 is confirmed. The waiting period enhances the security of the transactions included in block 2056 but still exploitable. If a merchant releases goods instantly or just after a confirmation might not receive the money if block 2056 is affected being an orphaned block or compromised by other attacking methods. However, we show that PoAj does all its verification prior to a block is affixed as a confirmed block to the main chain and also stimulates faster transactions of large-sized lower fees transactions. Hence, it allows merchants to release goods as soon as 1 confirmation, the final confirmation, received from the main chain.

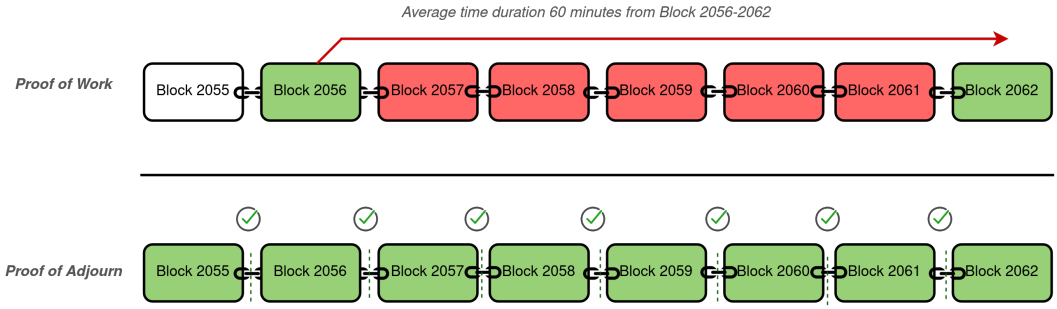

Figure 9. The top chain shows an example where new added blocks in PoW need to wait for 6 block confirmation. The chain at the bottom uses PoAj and do not need to wait for any confirmation block.

7.4. Selfish Mining

Due to the centralization aspect of the bitcoin mining pools, miners can put a huge impact on many aspects of a cryptocurrency. Selfish mining is one of such aspects that can affect the network badly. Research shows that only 6 mining pools were able to generate about 67% of the total bitcoin blocks in a 24-h period. The research also suggests that during that period the pools were able to generate 2 or more blocks in a sequence several times proving their ability of selfish mining [6]. This is a very alarming scenario for the rest of the network nodes, as well as the cryptocurrency participants.

PoAj approach mitigates the problem of selfish mining regardless of the mining ability of any miner. A selfish miner may choose to generate blocks in secret but not propagate the blocks to the network nodes. While the selfish miner finds more blocks to lead the main chain, he broadcast the blocks to the network that results in the rivalries losing any mining reward already received along with the discarded block. PoAj security approach only accepts block with (+1) height, hence a selfish miner will not have the ability to discard its rivals blocks when producing more than 1 block in a sequence. Besides, the PoAj verification check also includes a Block generation time check. Hence, any blocks which have been hiding for a longer period will not pass this check, as well. Only the most recent blocks that are mined within the set threshold time, passes the verification.

Figure 10 shows that a selfish miner in PoW is able to discard its rivals mined blocks by forcing them to lose all their reward, whereas, in a similar scenario at PoAj, attacker's mined block does not pass the verification process for being hidden longer than the threshold time and also not meeting the conditions.

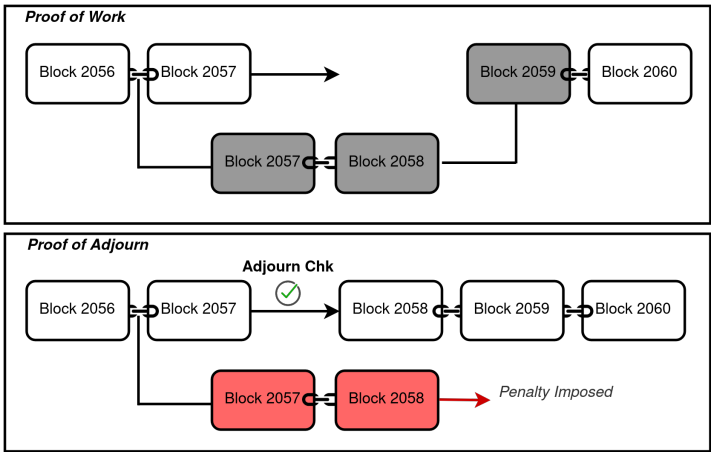

Figure 10. The top chain shows a selfish miner attacker in PoW where legitimate blocks are discarded (2057). The chain at the bottom is PoAj where the attack is mitigated.

7.5. Summary

The evaluation of the major attacks against the proposed Proof of Adjourn (PoAj) showed that PoAj is an effective consensus approach that can mitigate the 5 major attacks analyzed in the paper, as well as reduce the transaction processing time of large-sized transactions. Table 1 summarizes the attacks that PoAj can mitigate compared to PoW, the current consensus protocol that is adopted in major cryptocurrencies.

Table 1. The effectiveness of PoAj compared to current approach.

Attack Techniques	Mitigates Attacks	
	PoW	PoAj
51% Attack	✗	✓
Selfish Mining Attack	✗	✓
Miner Bribe Attack	✗	✓
Zero Confirmation Attack	✗	✓
One Confirmation Attack	✗	✓

8. Conclusions

The majority hash rate issue has been a serious problem that has jeopardized blockchain networks. One of the weak attributes of PoW based cryptocurrencies is the longest chain-rule. Hence, many cryptocoins with low hashing are under a constant high risk of exploitation.

In this paper, we focused on the current and future challenges of blockchain. We discussed 5 major attacks and showed that the current protection techniques fail to provide enough protection, leaving this technology exposed to attackers. To overcome all problems, we proposed Proof of Adjourn (PoAj), a novel consensus protocol that mitigates the 51% Attack, Selfish Mining, Miner Bribe Attack, Zero Confirmation Attack, One Confirmation Attack, and Transaction Confirmation Delay issue.

The main strength of PoAj is that it provides enough protection regardless of attackers hashing ability and also solves the immense waiting time issue enhancing faster transactions of large-sized transactions. For this reason, PoAj is not only an effective protection mechanism for current attacks, but it is also able to deter future attacks based on hashing power.

Author Contributions: Writing—original draft, S.S. and H.M.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mearian, L. What Is Blockchain? The Complete Guide. 2019. Available online: https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html (accessed on 17 March 2020).
2. Miles, C. Blockchain Security: What Keeps Your Transaction Data Safe? 2017. Available online: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/ (accessed on 17 March 2019).
3. Teruel, M.A.; Trujillo, J. Easing ĐApp Interaction for Non-Blockchain Users from a Conceptual Modelling Approach. *Appl. Sci.* **2020**, *10*, 4280. [CrossRef]
4. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci* **2019**, *9*, 2400. [CrossRef]
5. Sarwar, S.; Hector, M.-G. On the Effectiveness of Blockchain Against Cryptocurrency Attacks. *IARIA* **2018**, *2018*, 2308–4278.
6. Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]

7. BitDegree. Understanding the Different Types of Cryptocurrency. 2020. Available online: https://www.bitdegree.org/tutorials/types-of-cryptocurrency/ (accessed on 17 March 2020).
8. Rizun, P.R. The Excessive-Block Gate: How a Bitcoin Unlimited Node Deals With Large Blocks. 2016. Available online: https://medium.com/@peter_r/the-excessive-block-gate-how-a-bitcoin-unlimited-node-deals-with-large-blocks-22a4a5c322d4 (accessed on 20 January 2019).
9. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Technical Report; Manubot. 2019. Available online: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed on 20 November 2019).
10. Dinkins, D. Satoshi's Best Kept Secret: Why Is There a 1 MB Limit to Bitcoin Block Size. 2017. Available online: https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size (accessed on 31 August 2020).
11. Phillips, D. Bitcoin Network Slows Down as the Mempool Builds. 2020. Available online: https://decrypt.co/29619/bitcoin-network-slows-down-as-the-mempool-builds (accessed on 31 August 2020).
12. Tuwiner, J. Bitcoin Confirmations. 2020. Available online: https://www.buybitcoinworldwide.com/confirmations/ (accessed on 31 August 2020).
13. Sayeed, S.; Marco-Gisbert, H.; Caira, T. Smart Contract: Attacks and Protections. *IEEE Access* **2020**, *8*, 24416–24427. [CrossRef]
14. Pearson, J. A Major Bug in Bitcoin Software Could Have Crashed the Currency. 2018. Available online: https://www.vice.com/en_us/article/qvakp3/a-major-bug-in-bitcoin-software-could-have-crashed-the-currency (accessed on 17 March 2020).
15. Partz, H. Bitcoin Core Update Fixes Vulnerability That Reportedly Could Crash Network for $80,000. 2018. Available online: https://cointelegraph.com/news/bitcoin-core-update-fixes-vulnerability-that-reportedly-could-crash-network-for-80-000 (accessed on 17 March 2020).
16. Alsayed Kassem, J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
17. Sharma, T.K. Public vs. Private Blockchain: A Comprehensive Comparison. 2019. Available online: https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (accessed on 12 March 2020).
18. Anderson, M. Exploring Decentralization: Blockchain Technology and Complex Coordination. 2019. Available online: https://jods.mitpress.mit.edu/pub/7vxemtm3/release/2 (accessed on 17 February 2020).
19. Buterin, V. The Meaning of Decentralization. 2017. Available online: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed on 10 April 2020).
20. James Royal, .K.V. What Is Cryptocurrency? Here's What You Should Know. 2019. Available online: https://www.nerdwallet.com/blog/investing/cryptocurrency-7-things-to-know/ (accessed on 17 March 2020).
21. Mcintosh, S. The Business Benefits of Cryptocurrency. 2018. Available online: https://www.theglobaltreasurer.com/2018/08/08/the-business-benefits-of-cryptocurrency/ (accessed on 10 September 2019).
22. Reiff, N. Blockchain Explained. 2020. Available online: https://www.investopedia.com/terms/b/blockchain.asp (accessed on 10 March 2020).
23. Blockchain.com. Bitcoin Transaction Fees: What Are They & Why Should You Care? 2016. Available online: https://medium.com/blockchain/bitcoin-transaction-fees-what-are-they-why-should-you-care-6c7347e6f5d6 (accessed on 12 March, 2019).
24. Katalyse.io. Blockchain Basics—What Is Masternode. 2018. Available online: https://cryptodigestnews.com/blockchain-basics-what-is-masternode-dbed481a846e (accessed on 19 March 2019).
25. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
26. Joshi, N. 8 Blockchain Consensus Mechanisms You Should Know About. 2019. Available online: https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about (accessed on 11 November 2019).
27. The Delegated Proof of Stake (DPOS) Explained. 2018. Available online: https://www.tokens24.com/cryptopedia/basics/delegated-proof-stake-dpos-explained (accessed on 11 July 2019).
28. Frankenfield, J. Proof of Stake (PoS). 2019. Available online: https://www.investopedia.com/terms/p/proof-stake-pos.asp (accessed on 12 February 2020).

29. Budiman, J. What Is a Merkle Tree and How Does It Help Organize Data On The Bitcoin Blockchain? 2018. Available online: https://bitcoin.co.uk/what-is-a-merkle-tree-and-how-does-it-help-organize-data-on-the-bitcoin-blockchain/ (accessed on 19 January 2020).
30. Blockgeeks. The Best Step-by-Step Bitcoin Script Guide. 2018. Available online: https://blockgeeks.com/guides/best-bitcoin-script-guide/ (accessed on 12 April 2020).
31. Sun, F. UTXO vs Account/Balance Model. 2018. Available online: https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf (accessed on 12 April 2020).
32. Cointelegraph. What Is Lightning Network And How It Works. 2020. Available online: https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works (accessed on 12 April 2020).
33. Konstantopoulos, G. Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance. 2017. Available online: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419 (accessed on 10 November 2018).
34. Suberg, W. Phishing Attack on Electrum Wallet Nets Hacker Almost $1 Million in Hours: Report. 2018. Available online: https://cointelegraph.com/news/phishing-attack-on-electrum-wallet-nets-hacker-almost-1-million-in-hours-report (accessed on 12 January 2020).
35. Property2chain. The Double Spending Problem in Real Estate Transactions. 2018. Available online: https://medium.com/@property2chain/the-double-spending-problem-in-real-estate-transactions-fecdf1d9ce79 (accessed on 12 January 2020).
36. Bitcoin.com. What is Bitcoin Double-Spending? 2017. Available online: https://www.bitcoin.com/info/what-is-bitcoin-double-spending (accessed on 12 January 2019).
37. Shanmugam, K. Centralized vs Decentralized Cryptocurrency Exchanges—Explained Simply! 2019. Available online: https://hackernoon.com/centralized-vs-decentralized-cryptocurrency-exchanges-explained-simply-639411ecb452 (accessed on 17 April 2020).
38. Paganini, P. Group-IB: 14 Cyber Attacks on Crypto Exchanges Resulted in a Loss of $882 Million. 2018. Available online: https://securityaffairs.co/wordpress/77213/hacking/cyber-attacks-crypto-exchanges.html (accessed on 16 April 2020).
39. Nasdaq. Byzantine Fault Tolerance: The Key for Blockchains. 2017. Available online: https://www.nasdaq.com/articles/byzantine-fault-tolerance-key-blockchains-2017-06-29 (accessed on 12 April 2019).
40. Rosic, A. What Is Hashing? 2017. Available online: https://blockgeeks.com/guides/what-is-hashing/ (accessed on 19 September 2018).
41. Rilcoin. Cryptocurrency Hash and the Difference Between Sha and Scrypt. 2017. Available online: https://medium.com/@rilcoin/cryptocurrency-hash-and-the-difference-between-sha-and-scrypt-1f2217eb5b89 (accessed on 15 April 2019).
42. HIMSS. Cryptography in Blockchain. 2019. Available online: https://www.himss.org/resources/cryptography-blockchain (accessed on 12 April 2019).
43. Risberg, J. Verge Falls Victim to 51% Attack, Again. 2020. Available online: https://coincentral.com/verge-falls-victim-to-51-attack-again/ (accessed on 31 August 2020).
44. Zimwara, T. Ethereum Classic Suffers 51% Attack Again: Delisting Risk Amplified. 2020. Available online: https://news.bitcoin.com/ethereum-classic-suffers-51-attack-again-delisting-risk-amplified/ (accessed on 31 August 2020).
45. Martin, J. Bitcoin Gold Blockchain Hit by 51% Attack Leading to $70K Double Spend. 2020. Available online: https://cointelegraph.com/news/bitcoin-gold-blockchain-hit-by-51-attack-leading-to-70k-double-spend (accessed on 19 April 2020).
46. Komodo. Komodo's Blockchain Security Service. 2019. Available online: https://komodoplatform.com/wp-content/uploads/2019/02/Komodo-Blockchain-Security-Service-Brochure.pdf (accessed on 12 March 2019).
47. Matt. Bitcoin's Attack Vectors: 51% Attacks, 2018. Available online: https://medium.com/chainrift-research/bitcoins-attack-vectors-51-attacks-a96deac43774 (accessed on 11 January 2019).
48. Rosenfeld, M. Analysis of Hashrate-Based Double Spending. *arXiv* **2014**, arXiv:1402.2009.
49. Bai, Q.; Zhou, X.; Wang, X.; Xu, Y.; Wang, X.; Kong, Q. A Deep Dive into Blockchain Selfish Mining. *arXiv* **2018**, arXiv:1811.08263.
50. Vitalik, B. Selfish Mining: A 25% Attack Against the Bitcoin Network. 2013. Available online: https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/ (accessed on 17 August 2018).

51. Tuwiner, J. Bitcoin Mining in China. 2020. Available online: https://www.buybitcoinworldwide.com/mining/china/ (accessed on 31 August 2020).
52. Peter, R. Empirical Double spend Probabilities for Unconfirmed Transactions, 2018. Available online: https://satoshisvisionconference.com/ (accessed on 12 March 2019).
53. Pérez-Solà, C.; Delgado-Segura, S.; Navarro-Arribas, G.; Herrera-Joancomartí, J. Double-spending prevention for Bitcoin zero-confirmation transactions. *Int. J. Inf. Secur.* **2017**, *18*, 1–13. [CrossRef]
54. Nikolov, T. 0-Conf Series. Part 1: Support for Zero-Confirmation Transactions at Bitcoin ATM. to be, or Not to be. 2019. Available online: https://coinatmradar.com/blog/support-zero-confirmation-transactions-at-bitcoin-atm/ (accessed on 31 August 2020).
55. Judmayer, A.; Stifter, N.; Krombholz, K.; Weippl, E.R. Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms. *Synth. Lect. Inf. Secur. Privacy Trust.* **2017**, *9*, 1–123. [CrossRef]
56. Cryptonews. Countries Where Bitcoin Is Banned or Legal In 2020. 2020. Available online: https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm (accessed on 31 August 2020).
57. Huang, R. China's Proposal To Ban Cryptocurrency Mining Has Little To Do With The Environment. 2019. Available online: https://www.forbes.com/sites/rogerhuang/2019/04/25/chinas-move-to-ban-cryptocurrency-mining-has-little-to-do-with-the-environment/#285f10ed46ed (accessed on 19 March 2020).
58. Rudden, J. Bitcoin Market Capitalization Quarterly 2013–2020. 2020. Available online: https://www.statista.com/statistics/377382/bitcoin-market-capitalization/ (accessed on 10 July 2020).
59. Alberto, G.; Pier, S.; Robert, V.; Uri, S. A penalty System for Delayed Block Submission, 2018. Available online: https://www.horizen.global/assets/files/A-Penalty-System-for-Delayed-Block-Submission-by-Horizen.pdf (accessed on 17 January 2019).
60. ChainZilla. Blockchain Security and How to Mitigate. 2019. Available online: https://medium.com/chainzilla/solutions-to-51-attacks-and-double-spending-71526be4bb86 (accessed on 12 February 2019).
61. Fawkes. PirlGuardInnovative Solution against 51% Attacks. 2018. Available online: https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-87dd45aa1109 (accessed on 19 January 2019).
62. Alexander, B. Mitigating 51% attacks with LLMQ-based ChainLocks, 2018. Available online: https://blog.dash.org/mitigating-51-attacks-with-llmq-based-ChainLocks-7266aa648ec9 (accessed on 7 March 2019).
63. Edmund, N.G. A Dash to Mitigate 51% Attacks with ChainLocks. 2018. Available online: https://blockchainreporter.net/2018/12/01/dash-to-mitigate-51-attacks-with-ChainLocks/ (accessed on 12 January 2019).
64. Nicehash. Largest Crypto Mining Marketplace. 2014. Available online: https://www.nicehash.com/ (accessed on 13 August 2019).
65. Cryptocompare.com. What Is Merged Mining-Bitcoin & Namecoin-Litecoin & Dogecoin. 2015. Available online: https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/ (accessed on 14 January 2019).
66. BiXBit. Merged Mining—collective Benefit and a Panacea for 51% Attack? 2018. Available online: https://medium.com/@bixbit.official/merged-mining-collective-benefit-and-a-panacea-for-51-attack-373404106a9 (accessed on 31 August 2020).
67. Solat, S.; Potop-Butucaru, M.G. ZeroBlock: Preventing Selfish Mining in Bitcoin. *arXiv* **2016**, arXiv:1605.02435.